UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF PENNSYLVANIA

IN RE WAWA, INC. DATA SECURITY LITIGATION	**Case No. 2:19-CV-06019** **CONSOLIDATED AMENDED CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**
This Document Relates to All Financial Institution Track Cases	

Plaintiffs Inspire Federal Credit Union, Insight Credit Union, and Greater Cincinnati Credit Union ("Plaintiffs"), on behalf of themselves and all others similarly situated, assert the following against Defendant Wawa, Inc. (collectively, "Wawa" or "Defendant"), based upon personal knowledge, where applicable, information and belief, and the investigation of counsel.

I. INTRODUCTION

1. Plaintiffs bring this class action on behalf of financial institutions that issue payment cards and that suffered, and continue to suffer, financial losses as a direct result of Wawa's conscious failure to take adequate and reasonable measures to protect its point-of-sale ("POS") payment terminals, fuel dispensers, and payment processing servers.

2. In March 2019, hackers exploited Wawa's deficient security measures to access Wawa's POS system and installed malicious software ("malware") that infected Wawa's in-store payment terminals and fuel dispensers. This malware allowed hackers to steal highly sensitive information, including, but not limited to, cardholder names, credit and debit card numbers, and

expiration dates ("Payment Card Data"), from transactions that Plaintiffs' members entered at Wawa from at least March 4, 2019 through December 12, 2019 (the "Data Breach").

3. Payment Card Data acquired during the Data Breach started to become available for sale on the "dark web" shortly thereafter. In January 2020, hackers posted "fresh" information for over 30 million payment cards in a package titled the "BIGBADABOOM-III" to the underground website the "Joker's Stash." Cybersecurity experts were quickly able to identify the Payment Card Data published on Joker's Stash as originating from cards that were used at Wawa. This Payment Card Data included information associated with cards issued by Plaintiffs.

4. The Data Breach was the foreseeable (and inevitable) result of Wawa's inadequate data security measures and lackadaisical approach to the security of its customers' Payment Card Data. Merchants like Defendant have been warned by the major card brands (e.g., Visa) about the exact kind of "RAM scraper" malware at the center of the Data Breach since at least 2009.[1] Moreover, as explained below, Wawa refused to implement certain best practices, failed to upgrade critical security systems, used outdated POS systems, ignored warnings about the vulnerability of its computer network, and disregarded and/or violated applicable industry standards despite the well-publicized and ever-growing threat of cyber-attacks targeting Payment Card Data through vulnerable POS systems and inadequately protected computer networks.

5. The damages caused by Wawa's data security deficiencies were further exacerbated by its failure to timely identify the Data Breach and subsequently contain it. By December 19, 2019, when Wawa first publicly acknowledged that a data breach compromising customer

[1] Adam Tyler, *The Low Cost and High Reward of POS Malware*, CSID, at 2, https://www.experianpartnersolutions.com/wp-content/uploads/2017/01/WP_POSMalware_2014.pdf (last visited July 13, 2020) ("In 2009, Visa and Verizon published threat reports outlining a new type of malware called a RAM scraper.").

Payment Card Data had occurred, the Data Breach had already been ongoing for at least nine months.

6. As payment card issuers, Plaintiffs are required by regulation to reimburse payment card account holders (i.e., the persons whose Payment Card Data was stolen during the Data Breach) for fraudulent or unauthorized charges made to their account. Accordingly, Plaintiffs have and will continue to incur significant damages as a result of the Data Breach including, *inter alia*, costs to cancel and reissue the payment cards compromised in the Data Breach, costs to refund fraudulent charges which occur on the compromised payment cards prior to their cancellation and reissuance, costs to investigate such fraudulent charges, costs to monitor the compromised card accounts, and loss of revenue (e.g., interest and transaction fees) resulting from decreased card usage. Plaintiffs are also at a substantial risk of suffering harm from fraudulent charges made to cards that were compromised in the Data Breach, unless such cards are cancelled and replaced. Further, the risk of additional future harm remains in the likely event that additional Payment Card Data stolen in the Data Breach is made available on the dark web.

II. PARTIES

A. Plaintiffs

7. Plaintiff Inspire Federal Credit Union is a citizen of the Commonwealth of Pennsylvania. Plaintiff is a federally chartered credit union with its principal place of business located in Newtown, Pennsylvania. Plaintiff Inspire received a "fraud alert" from Visa and/or MasterCard (the "Card Brands"), which identified payment cards it had issued as having been compromised in the Data Breach. Consistent with payment card industry best practices, as well as those enunciated by the Card Brands, Plaintiff Inspire has incurred costs to mitigate the risk of fraudulent activity on the payment card accounts compromised in the Data Breach. As a direct

result of the Wawa Data Breach, Plaintiff Inspire Federal Credit Union has suffered, and continues to suffer, injury, including, *inter alia*, costs to cancel and reissue cards compromised in the Data Breach, costs to refund fraudulent charges, costs to investigate fraudulent charges, costs to monitor impacted cards, and costs due to lost interest and transaction fees due to reduced card usage.

8. Plaintiff Insight Credit Union is a citizen of the State of Florida. Plaintiff is a state chartered credit union with its principal place of business located in Orlando, Florida. Plaintiff Insight received a "fraud alert" from Visa and/or MasterCard, which identified payment cards it had issued as having been compromised in the Data Breach. Consistent with payment card industry best practices, as well as those enunciated by the Card Brands, Plaintiff Insight has incurred costs to mitigate the risk of fraudulent activity on the payment card accounts compromised in the Data Breach. As a direct result of the Wawa Data Breach, Plaintiff has suffered, and continues to suffer, injury, including, *inter alia*, costs to cancel and reissue cards compromised in the Data Breach, costs to refund fraudulent charges, costs to investigate fraudulent charges, costs to monitor impacted cards, and costs due to lost interest and transaction fees due to reduced card usage.

9. Plaintiff Greater Cincinnati Credit Union is a citizen of the State of Ohio. Plaintiff is a federally charted credit union with its principal place of business located in Cincinnati, Ohio. Plaintiff Greater Cincinnati Credit Union received a "fraud alert" from Visa and/or MasterCard, which identified payment cards it had issued as having been compromised in the Data Breach. Consistent with payment card industry best practices, as well as those enunciated by the Card Brands, Plaintiff Greater Cincinnati Credit Union has incurred costs to mitigate the risk of fraudulent activity on the payment card accounts compromised in the Data Breach. As a direct result of the Wawa Data Breach, Plaintiff Greater Cincinnati Credit Union has suffered, and continues to suffer, injury, including, *inter alia*, costs to cancel and reissue cards comprised in the

Data Breach, costs to investigate fraudulent charges, costs to monitor impacted cards, and costs due to lost interest and transaction fees due to reduced card usage.

10. Additionally, Plaintiffs remain at substantial risk of suffering additional harm as a direct result of the Data Breach. For example, to the extent any payment cards compromised in the Data Breach have not been canceled and reissued, Plaintiffs continue to face an imminent risk of suffering losses resulting from fraudulent transactions made to those members' cards. Further, Wawa's shortcoming in preventing, detecting, and responding to the Data Breach were so inadequate that there is a significant risk that Wawa failed to cure the deficiencies in its data security measures in a manner sufficient to prevent a subsequent data breach.

B. Defendant

11. Defendant Wawa, Inc. is a New Jersey corporation with its principal place of business in this District in Wawa, Pennsylvania.

12. Wawa is engaged in the business of developing and operating a system of convenience stores. Wawa currently operates more than 850 retail stores throughout Pennsylvania, New Jersey, Delaware, Maryland, Virginia, Florida, and Washington, D.C. Wawa offers gasoline at over 600 of these locations.[2] Wawa serves approximately 800 million customers each year.

13. Wawa is not a franchisor. It has total control over the manner in which its more than 850 locations operate, including information security at those locations, the computer software and electronic data transmission systems utilized to process payment card transactions, and how sensitive Payment Card Data is processed.

[2] *About Wawa*, WAWA, https://www.Wawa.com/about (last visited July 13, 2020).

III. JURISDICTION AND VENUE

14. This Court has jurisdiction over this action pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d), because at least one Class member is of diverse citizenship from one Defendant (e.g., Insight Credit Union), there are more than 100 Class members, and the aggregate amount in controversy exceeds $5 million, exclusive of interest and costs (e.g., the estimated cost to reissue the 30 million cards compromised by the Data Breach alone is in the tens of millions of dollars).

15. This Court has personal jurisdiction over Defendant named in this action because Wawa is headquartered within, and conducts substantial business in, Pennsylvania and this District through its convenience stores and commercial website.

16. Venue is proper in this District under 28 U.S.C. § 1391(b) because Defendant is headquartered in this District and a substantial part of the events, errors, omissions, and decisions leading up to the Data Breach occurred in this District.

IV. FACTUAL ALLEGATIONS

A. Payment Card Processing Background

17. Like many merchants, a large portion of Wawa's sales are made to customers who use credit or debit cards. When a customer uses a credit or debit card, the transaction involves four primary parties: (1) the "merchant" (e.g., Wawa) where the purchase is made; (2) an "acquiring bank" (which typically is a financial institution that contracts with the merchant to process its payment card transactions); (3) a "card network" or "payment processor" (such as Visa and MasterCard); and (4) the "issuer" (which is a financial institution—such as Plaintiffs—that issues credit and debit cards to its members/customers).

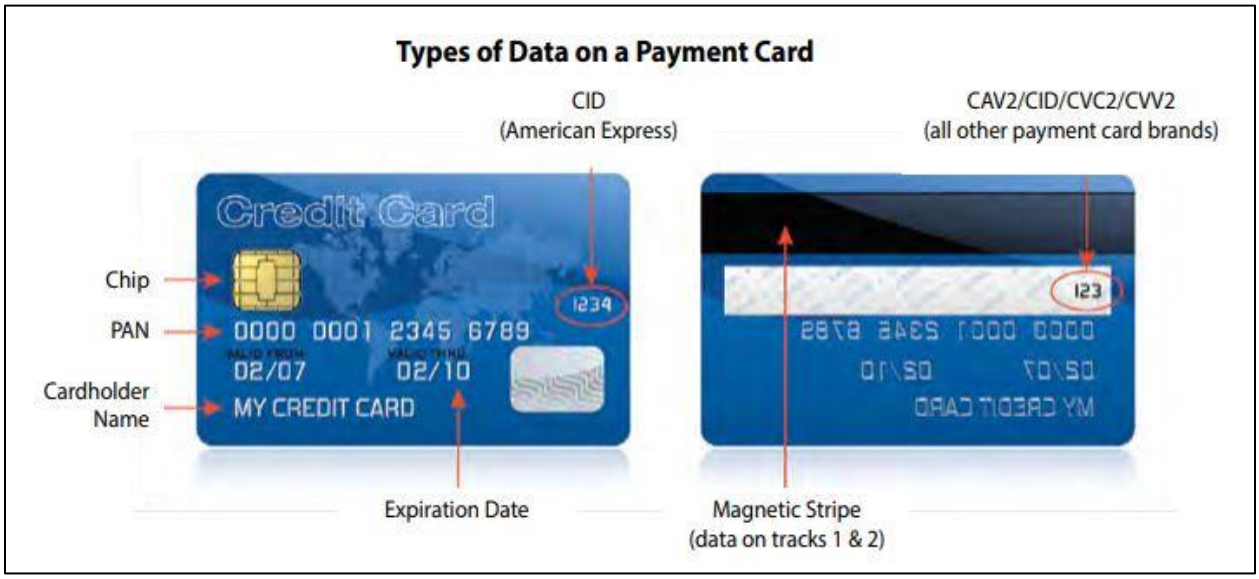
18. Processing a payment card transaction involves four major steps:

- *Authorization* – when a customer presents a card to make a purchase, Wawa requests authorization of the transaction from the card's issuer;
- *Clearance* – if the issuer authorizes the transaction, Wawa completes the sale to the customer and forwards a purchase receipt to the acquiring bank with which it has contracted;
- *Settlement* – the acquiring bank pays Wawa for the purchase and forwards the receipt to the issuer, which then reimburses the acquiring bank; and
- *Post-Settlement* – the issuer posts the charge to the customer's credit or debit account.

19. In processing payment card transactions, merchants gain access to and transmit a substantial amount of information about each customer, including his or her full name; credit or debit card account number (the "Primary Account Number" or "PAN"); card security code or verification value (referred to as the "CID" or "CAV2", "CVC2", or "CVV2" depending on the card brand) used to validate card information during the authorization process; the card's expiration date; and the PIN number for debit cards.[3] This information is typically stored in the magnetic stripe on the back of the payment card in two "tracks" (referred to as "Track 1" and "Track 2"), which are read when the customer swipes their card at a payment terminal.

[3] *See* PCI SEC. STANDARDS COUNCIL, PCI DSS QUICK REFERENCE GUIDE: UNDERSTANDING THE PAYMENT CARD INDUSTRY DATA SECURITY STANDARD VERSION 3.2.1, at 11, (July 2018), https://www.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf.

FIGURE 1



20. As described above, this information passes through the merchants' computer systems as it is transmitted to third parties, which is necessary to complete a transaction. At other times, and for other reasons, merchants may also collect other personally identifiable information about their customers, including, but not limited to, financial data, mailing addresses, phone numbers, driver's license numbers, and email addresses.

21. However, not all of this information is required to commit fraud. Hackers can make fraudulent charges with only some of the Payment Card Data described above. Indeed, fifteen state attorney generals, including the Pennsylvania Attorney General, have confirmed that identity thieves can enter fraudulent transactions without the card security code or verification value.[4]

22. To reduce vulnerabilities associated with swipe-only processing, the payment card industry developed EMV chip technology, which uses a computer chip embedded on a payment card. At the point of sale, the card is "dipped" into a chip reader—rather than swiped—and a

[4] Eric T. Schneiderman, Joint Letter, *RE: Aptos Communications with Client-Retailers Resulting from Data Breach*, (June 5, 2017), https://www.law360.com/articles/934951/attachments/0.

unique code is generated during the transaction. This technology makes it significantly more difficult for a would-be fraudster to create counterfeit cards using stolen payment card data. Nevertheless, Wawa continued to use magnetic stripe technology even though Card Brands and industry experts warned that the use of such outdated technology presented a significant risk of attack.

23. Wawa has obtained massive amounts of customer Payment Card Data over the years. Wawa uses this information to process payment card transactions in connection with sales to its customers. Customer Payment Card Data is an asset of considerable value to both Wawa and to hackers, who can easily sell this data, as a result of the "proliferation of open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce."[5]

24. Wawa is—and at all relevant times has been—aware that the Payment Card Data that it obtains and processes is highly sensitive and could be used for nefarious purposes by third parties, such as perpetrating identity theft and making fraudulent purchases. To this end, Wawa posted a job opening on or about December 4, 2019—just days before allegedly discovering the Wawa Data Breach—seeking an Information Security Incident Response Junior Analyst to "follow the processes and procedures necessary for the detection, response and remediation of cyber related attacks on the Wawa enterprise."[6]

25. Wawa also is—and at all relevant times has been—aware of the importance of safeguarding its customers' Payment Card Data and of the foreseeable consequences that would occur if its data security systems were breached, including the fraud losses and theft that would be

[5] *The Value of a Hacked Company*, KREBSONSECURITY (July 16, 2016), http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/.

[6] Wawa, *Wawa Information Security Incident Response Junior Analyst*, INDEED, (Dec. 3, 2019), https://www.indeed.com/viewjob?jk=7a1f2ac3eeb48eea&tk=1dsibai40p2p0800&from=serp&vjs=3 (copy saved by Plaintiffs' counsel).

imposed on consumers, and, ultimately, entities such as Plaintiffs. Indeed, given the extensive network of financial institutions involved in these transactions and the sheer volume of daily transactions using credit and debit cards, financial institutions and credit card processing companies have issued rules and standards governing the basic measures and protections that merchants must take to ensure consumers' valuable data is protected. This includes "Card Operating Regulations" which generally prohibit Defendant (or any merchant) from disclosing any cardholder account numbers, personal information, magnetic stripe information, or transaction information to third parties other than the merchant's agent, the acquiring bank, or the acquiring bank's agents. Under the Card Operating Regulations, Defendant is required to maintain the security and confidentiality of debit and credit cardholder information and magnetic stripe information and protect it from unauthorized disclosure.

26. Not surprisingly, Wawa's December 4, 2019 job posting also required the successful applicant have a "[v]ery basic understanding of relevant legal and regulatory requirements, such as: Payment Card Industry Data Security Standard."[7]

27. In addition to its independent duty to act reasonably in handling and safeguarding customers' Payment Card Data to prevent the foreseeable risk of future harm to others, Wawa is—and at all relevant times has been—obligated to safeguard such information by, among other things, industry standards, federal law, and its own commitments, internal policies, and procedures.

B. Wawa Was on Notice of Its Security Vulnerabilities and the Risk that Payment Card Information Would Be Compromised

28. Wawa knew or should have known that customer Payment Card Data is valuable and that hackers would target its POS systems to obtain such information. In 2014, retail entities

[7] *Id.*

not only surpassed credit, banking and financial institutions as the leader in greatest number of data breaches experienced per year and by far. The trend continued, with US retailers *leading the world* in data breaches as of 2018.[8] The most common means of data theft was through hacking, phishing, or skimming schemes targeting POS systems—the same techniques employed here.[9] Indeed, in 2015 alone, approximately 64% of all retail industry data breaches involved infiltrating companies' POS systems.[10]

29. Wawa's breach was foreseeable because data breaches involving numerous businesses, including Neiman Marcus, Michaels, Sally Beauty Supply, P.F. Chang's China Bistro, Eddie Bauer, Goodwill, SuperValu Grocery, UPS, Home Depot, Jimmy John's, Dairy Queen Restaurants, Staples, Kmart, Noodles & Co., GameStop, Wendy's, Chipotle, and Arby's, have all been widely reported by the media over the last several years. These breaches have resulted in hundreds of millions of compromised payment cards,[11] and the number of breaches only continues to increase each year.[12]

30. Moreover, each of these POS system breaches, like the Wawa Data Breach, involved a common kind of RAM "scraper" malware that extracts payment information from infected POS systems by grabbing "track" data—which is embedded in the magnetic stripe tracks on back of payment cards—that is read with each swipe and routed for processing. Notably, Visa

---

[8] Dan Alaimo, *US Retailers lead world in data breaches*, RETAIL DIVE (July 30, 2018), https://www.retaildive.com/news/us-retailers-lead-world-in-data-breaches/528873/.

[9] *Data Breaches Increase 40 Percent in 2016, Finds New Report from Identity Theft Resource Center and CyberScourt*, IDENTITY THEFT RESOURCE CENTER (Jan. 19, 2017), https://www.idtheftcenter.org/data-breaches-increase-40-percent-in-2016-finds-new-report-from-identity-theft-resource-center-and-cyberscout/.

[10] *2016 Data Breach Investigations Report*, VERIZON, at 25 (2016), https://enterprise.verizon.com/resources/reports/2016/DBIR_2016_Report.pdf.

[11] *A Special Report on Attacks on Point-of-Sale Systems*, SYMANTEC, at 3 (Nov. 20, 2014), https://docs.broadcom.com/doc/attacks-on-point-of-sale-systems-en.

[12] *See* IDENTITY THEFT RESOURCE CENTER, *supra* note 9.

(which Wawa accepts) explicitly warned convenience store chains that operate gas stations (including Wawa) of RAM scraper malware for magnetic stripe data at least as early as May 2009 in a Visa Data Security Alert.[13] Visa also repeatedly warned fuel merchants about the dangers of accepting magnetic stripe cards, providing specific recommendations, including the installation of EMV chip readers at fuel pumps prior to the Data Breach in November 2019.[14]

31. It was well known among retailers who accept payment cards, as well as data security professionals, that the same kind of RAM scraper malware deployed on Wawa's systems has been responsible for nearly every major data breach involving a POS system since 2013. This information alone put Wawa on notice that its POS systems would be targeted by hackers and that a data breach could lead to the theft of millions of customers' payment card information.

32. Wawa received additional warnings regarding malware infiltrations from other sources, including the U.S. Computer Emergency Readiness Team, a government unit within the Department of Homeland Security, which alerted retailers to the threat of POS malware on July 31, 2014, and issued a guide for retailers on protecting against the threat of POS malware, which was updated on August 27, 2014.[15] Wawa should have taken action to protect and ensure that its customers' information would not continue to be available to hackers and identity thieves, but Wawa chose not to do so.

33. Additionally, experts have long warned that the threat of hackers targeting POS systems is serious. Well-known security expert Michael Reitblat explained in a leading fast-casual

[13] Adam Tyler, *supra* note 1.

[14] Christian Hetrick, *'They were obviously not monitoring at an appropriate level': Before Wawa data breach, Visa warned it could happen*, THE MORNING CALL (Jan. 2, 2020), https://www.mcall.com/news/pennsylvania/mc-nws-pa-wawa-data-breach-20200102-sp2mm3eulneqhe6d7vbv56byse-story.html.

[15] *See* UNITED STATES COMPUTER EMERGENCY READINESS TEAM, ALERT (TA14-212A): BACKOFF POS MALWARE (Aug. 27, 2014), https://www.us-cert.gov/ncas/alerts/TA14-212A.

food industry trade publication that "[b]eyond POS systems, fraudsters often go directly to the source by attacking the restaurant's network or computer system, which stores files containing sensitive financial details. POS network attacks can affect multiple chain locations simultaneously and expose immense quantities of data in one fell swoop, allowing attackers to remotely steal data from each credit card as it is swiped at the cash register."[16] But, he noted that these data breaches are preventable: "[t]o help prevent fraud attacks, restaurants need to ensure they comply with the standards governing the handling of payment card information, . . . manage the risks associated with third party vendors and put an effective incident response plan into place."[17]

34. These warnings, among others, put Wawa on notice that it may be susceptible to a data breach and of the importance of prioritizing data security to prevent a breach. Despite Wawa's knowledge of the likelihood that its customers' payment card information would be stolen without reasonable security measures, and that its Cardholder Data Environment ("CDE") and POS systems were a target of hackers, Wawa failed to implement adequate data security measures that would have prevented hackers from penetrating its systems to steal Payment Card Data.

C. The Wawa Data Breach: March 2019 to Present

35. It is clear from Wawa's actions that it did not prioritize protecting customer Payment Card Data. Despite stating that "nothing is more important than honoring and protecting [our customers'] trust,"[18] Wawa's deficient data security measures left Payment Card Data for

[16] Michael Reitblat, *Is your restaurant data-breach proof?*, FAST CASUAL (Aug. 3, 2018), https://www.fastcasual.com/blogs/is-your-restaurant-data-breach-proof/.

[17] *Id.*

[18] *An Open Letter from Wawa CEO Chris Gheysens to Our Customers, Notice of Data Breach*, WAWA, https://s3.amazonaws.com/wawa-kentico-prod/wawa/media/misc/040220_databreach_openletter.pdf (last visited July 13, 2020).

every customer that shopped at its stores between at least March 4, 2019 and December 12, 2019, vulnerable to hackers who intend to, and did, use this information to commit fraud.

36. Up to, and including, the period during which the Wawa Data Breach occurred, Wawa's data security systems suffered from many deficiencies that made them susceptible to hackers, including, without limitation, the following:

a. Wawa's IT personnel were unqualified and failed to maintain a system of accountability over data security, thereby knowingly allowing data security deficiencies to persist;

b. Wawa ignored well-known warnings that its POS system was susceptible to a data breach (*see* Section IV.B., above);

c. Wawa failed to implement certain protocols that would have prevented unauthorized programs, such as malware, from being installed on its POS and other systems that accessed Payment Card Data and otherwise would have protected Payment Card Data. For example, not only did Wawa's anti-virus and anti-malware software (if any) fail to prevent the installation of the card-scraping malware at any of its locations, it likewise failed to identify the malware, allowing the Data Breach to continue for over nine months completely unnoticed. Whatever file integrity monitoring Wawa had in place wholly failed to detect the likely significant amount of suspicious activity ongoing at every one of Wawa's gas station and convenience store locations;

d. Wawa failed to install software to adequately track access to its network, monitor the network for unusual activity, and prevent exfiltration of data,

which would have detected the presence of hackers and prevented Payment Card Data from being stolen. Specifically, there are measures that are recommended and available to prevent data from leaving protected systems and from being sent to untrusted networks outside of the corporate systems. For example, IP whitelisting, which allows only specific IP addresses to connect to trusted corporate networks and networks within the CDE, prevents hackers from sending data outside the network even when they manage to identify and collect customers' sensitive data. Similarly, system information and event monitoring ("SIEM") programs are designed to track systems activity to look for suspicious connections and attempts to transfer files to or from untrusted networks; and

e. Wawa failed to properly train its employees about the risk of cyberattacks and how to mitigate them, including by failing to implement adequate security awareness training that would have instructed employees about the risks of common techniques, like "phishing" or social engineering, what to do if they suspect such attacks, and how to prevent them.

37. As a result of Wawa's security deficiencies, beginning at least as early as March 2019, computer hackers installed malware that infected potentially every Wawa location in the United States. Indeed, by April 22, 2019, the malware was on in-store and fuel pump payment systems at most of Wawa's 850 store locations.[19] Through this malware, the hackers were able to steal Payment Card Data that Wawa had collected in conjunction with its customers' purchases. With that Payment Card Data, these hackers were able to make undetected fraudulent purchases

[19] *Id.*

on credit and debit cards belonging to Plaintiffs' and Class members' customers, which Plaintiffs and the Class must ultimately reimburse. Hackers are also capable of specifically targeting and draining debit accounts with large amounts of money in them belonging to Plaintiffs' and Class members' customers.

38. Wawa also failed to timely identify the Data Breach. According to Wawa, it took until December 10, 2019 (approximately nine months after hackers first installed malware on its computer processors) to detect the breach and until December 19, 2019, to publicly report that "malware affected payment card information, including credit and debit card numbers, expiration dates, and cardholder names on payment cards used at potentially all Wawa in-store payment terminals and fuel dispensers."[20]

39. By failing to timely identify that its systems had been subjected to a data breach, Wawa gave hackers unfettered access to Wawa's computer and POS systems to obtain customers' Payment Card Data for more than nine months, thereby exponentially increasing the harm suffered by Plaintiffs and members of the Class.

40. The substantial scope and length of the Wawa Data Breach indicates Wawa's data security measures were woefully deficient. Indeed, Ron Schlecht, a data security expert at BTB Security wrote in January 2020: "What is most shocking to me, and should be most appalling to everybody, is how long this went undetected. How did Wawa just find this recently? They were obviously not monitoring at an appropriate level commensurate with their business volume and were unable to detect this anomalous activity."[21]

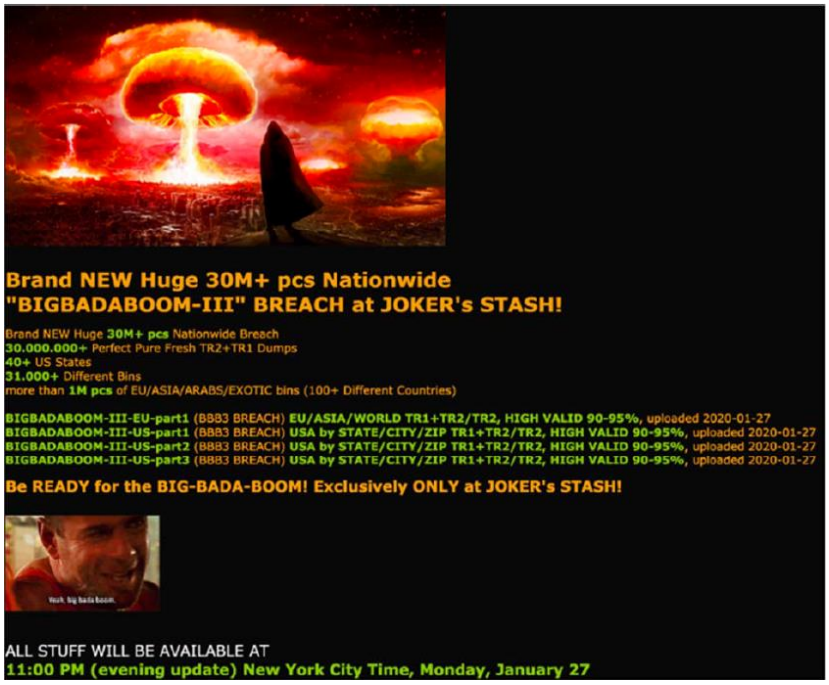
[20] *Id.*

[21] Christian Hetrick, *supra* note 14.

41. Plaintiffs first learned that they were affected by the Data Breach around December 27, 2019, for example, when Visa issued a series of Compromised Account Management System ("CAMS"), indicating that the estimated fraud "exposure window" for the Wawa Data Breach ran from April 22, 2019 through December 13, 2019. The CAMS alerts further indicated that both Track 1 and Track 2 data, which generally include credit and debit card information, such as cardholder name, primary account number, and expiration date may have been compromised in the Data Breach.

42. Furthermore, as a result of the Data Breach, on January 27, 2020 (after allegedly being locked out of Wawa's systems for over a month), hackers posted over 30 million payment cards on Joker's Stash, a website used to sell stolen payment cards to fraudsters. Figure 2 illustrates this screen shot:[22]

FIGURE 2



[22] *Wawa Breach May Have Compromised More than 30 Million Payment Cards*, KREBSONSECURITY (Jan. 28, 2020), https://krebsonsecurity.com/2020/01/wawa-breach-may-have-compromised-more-than-30-million-payment-cards/.

43. The Joker's Stash post above demonstrates the hackers successfully exfiltrated millions of Wawa's customers' Payment Card Data, resulting in the harm already sustained by Plaintiffs and Class Members, e.g., costs to reimburse fraudulent charges and other mitigation expenses. Additionally, the Joker's Stash post confirms that Plaintiffs and Class Members are at an imminent risk of future harm, including fraudulent charges that may be placed on customers' cards. While Wawa has not admitted that the cards posted to Joker's Stash came from its Data Breach, data security experts and financial institutions confirmed that the payment cards published on Joker's Stash were each used at a Wawa and the geographic mapping showed the cards were from locations where Wawa operates.[23] For example, Gemini Advisory, a New York-based fraud intelligence company noted that the largest concentration of stolen cards for sale in the BIGBADABOOM-III batch traced back to Wawa customers in Florida and Pennsylvania.[24] Gemini Advisory also noted that the "median price of US-issued records from this breach is currently $17, with some of the international records priced as high as $210 per card."[25]

44. Attempting to downplay the seriousness of the Data Breach, Wawa assured its customers that "anyone impacted [ ] will not be responsible for fraudulent charges related to this incident."[26] In a separate letter to customers, Wawa's CEO, Chris Gheysens wrote, "I want to reassure you that you will not be responsible for any fraudulent charges on your payment cards related to this incident[.]"[27] Notably missing from Wawa's communication was any mention of

[23] *Id.*

[24] Stas Alforov & Christopher Thomas, *Breached Wawa Payment Card Records Reach Dark Web*, GEMINI ADVISORY (Jan. 28, 2020), https://geminiadvisory.io/breached-Wawa-payment-card-records-reach-dark-web/.

[25] *Id.*

[26] *Wawa Notifies Customers of Data Security Incident*, Wawa (Dec. 19, 2019), https://s3.amazonaws.com/wawa-kentico-prod/wawa/media/misc/wawa-data-security-incident-wire-release-12_19_2019.pdf.

[27] *An Open Letter from Wawa CEO Chris Gheysens to Our Customers*, *supra* note 18.

the fact that Plaintiffs and Class members are the ones who, by regulation, are ultimately responsible for these fraudulent charges.

45. Wawa has not provided any assurances to Plaintiffs and similarly situated payment card issuers who will lose millions of dollars as a result of having to cancel and reissue cards compromised in the Wawa Data Breach, refund fraudulent charges incurred by their members/customers, investigate fraudulent charges, monitor accounts, and lose interest and transaction fees due to reduced card usage.

D. Wawa Failed to Comply with Its Duties

1. Wawa Failed to Comply with Industry Standards for Data Security

46. Wawa failed to comply with industry standards for data security and actively mishandled the data entrusted to it by its customers.

47. The Payment Card Industry Security Standards Council promulgates minimum standards, which apply to all organizations that store, process, or transmit Payment Card Data. These standards are known as the Payment Card Industry Data Security Standard ("PCI DSS"). PCI DSS is the industry standard governing the security of Payment Card Data, although it sets the minimum level of what must be done, not the maximum.

48. PCI DSS version 3.2.1 (as described in Figure 3, below), released in May 2018 and in effect at the time of the Wawa Data Breach, imposes the following 12 "high-level" mandates:[28]

[28] PCI SEC. STANDARDS COUNCIL, *supra* note 3.

FIGURE 3

The PCI Data Security Standard

PCI DSS is the global data security standard adopted by the payment card brands for all entities that process, store or transmit cardholder data and/or sensitive authentication data. It consists of steps that mirror security best practices.

Goals	PCI DSS Requirements
Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

49. Furthermore, PCI DSS 3.2.1 sets forth detailed and comprehensive requirements that have to be followed to meet each of the 12 mandates.

50. Among other things, PCI DSS 3.2.1 requires Wawa to: properly secure Payment Card Data; not store cardholder data beyond the time necessary to authorize a transaction; to timely upgrade its POS software; implement proper network segmentation; encrypt Payment Card Data at the POS; restrict access to Payment Card Data to those with a need to know; establish a process to identify; and timely fix security vulnerabilities. Upon information and belief, Wawa failed to comply with some or all of these requirements.

2. Wawa Failed to Comply with Federal Trade Commission Requirements

51. According to the Federal Trade Commission ("FTC"), the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act of 1914 ("FTC Act"), 15 U.S.C. § 45.

52. In 2007, the FTC published guidelines that establish reasonable data security practices for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vendor-approved patches to correct security problems. The guidelines also recommend that businesses consider using an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone may be trying to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

53. The FTC has also published a document entitled "FTC Facts for Business," which highlights the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.

54. The FTC has issued orders against businesses that have failed to employ reasonable measures to secure Payment Card Data. These orders provide further guidance to businesses regarding their data security obligations.

55. In the years leading up to the Wawa Data Breach, and during the course of the breach itself, Wawa failed to follow guidelines set forth by the FTC and actively mishandled the management of its IT security. Furthermore, by failing to have reasonable data security measures

in place, Wawa engaged in an unfair act or practice within the meaning of Section 5 of the FTC Act.

3. The Data Breach Damaged Financial Institutions

56. Wawa failed to protect its customers' Payment Card Data and as a result, Plaintiffs and Class members have and will suffer millions of dollars in damages.

57. Wawa failed to follow industry standards and failed to effectively monitor its POS and security systems to ensure the safety of customer information. Wawa's subpar security protocols, continued reliance on magnetic card stripe readers and acceptance of magnetic cards rather than EMV chip cards, improper retention of cardholder data, and failure to regularly monitor for unauthorized access caused customers' Payment Card Data to be compromised for months without detection by Wawa.

58. The Data Breach caused and/or will cause substantial damage to Plaintiffs and Class members, who acted immediately to mitigate the risk of a massive number of fraudulent transactions being made on payment cards that they issued while simultaneously taking steps to prevent future fraud. Consumers are ultimately protected from most fraud loss, but Plaintiffs and Class members are not. Financial institutions, like Plaintiffs and other Class members, bear primary responsibility for reimbursing members/customers for fraudulent charges and covering the cost of issuing replacement cards to members/customers to prevent future fraudulent charges caused by Wawa's failure to adopt adequate security measures.

59. As a result of the Wawa Data Breach, Plaintiffs and Class members are required, and will continue to be required, to cancel and reissue payment cards, change or close accounts, notify members that their cards were compromised, investigate claims of fraudulent activity, refund fraudulent charges, increase fraud monitoring on potentially impacted accounts, and take

other steps to protect themselves and their members/customers. Plaintiffs and members of the Class also lost or will lose interest and transaction fees due to reduced card usage. Furthermore, debit and credit cards belonging to Plaintiffs and Class members—as well as the account numbers on the face of the cards—were devalued.

60. The financial damages suffered by Plaintiffs and members of the Class are significant and ongoing.

V. CLASS ACTION ALLEGATIONS

61. Plaintiffs bring this action on behalf of themselves and as a class action, pursuant to the provisions of Rules 23(a), 23(b)(2), and 23(b)(3) of the Federal Rules of Civil Procedure, on behalf of the following class (the "Class"):

> All banks, credit unions, financial institutions, and other entities in the United States (including its Territories and the District of Columbia) that issued payment cards (including debit or credit cards) used by cardholders to make purchases from Wawa from March 4, 2019 to December 13, 2019.[29]

62. Excluded from the Class is Wawa and its subsidiaries and affiliates; all employees of Wawa; all persons who make a timely election to be excluded from the Class; government entities; and the judge to whom this case is assigned, including his/her immediate family and court staff.

63. Plaintiffs reserve the right to modify, expand or amend the above Class definitions or to seek certification of a class or subclasses defined differently than above before any court determines whether certification is appropriate following discovery.

64. Certification of Plaintiffs' claims for class-wide treatment is appropriate because all elements of Fed. R. Civ. P. 23(a) and (b)(2)-(3) are satisfied. Plaintiffs can prove the elements

[29] As evidence is developed, Plaintiffs may amend the class definition or class period if necessary, to accurately correspond to the relevant details of the Data Breach.

of their claims on a class-wide basis using the same evidence as would be used to prove those elements in an individual action alleging the same claims.

65. **Numerosity:** All requirements of Fed. R. Civ. P. 23(a)(1) are satisfied. The members of the Class are so numerous and geographically dispersed that individual joinder of all Class members is impracticable. While Plaintiffs are informed and believes that there are hundreds of members of the Class, the precise number of Class members is unknown to Plaintiffs. Class members may be identified through objective means. Class members may be notified of the pendency of this action by recognized, court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

66. **Commonality and Predominance:** All requirements of Fed. R. Civ. P. 23(a)(2) and 23(b)(3) are satisfied. This action involves common questions of law and fact, which predominate over any questions affecting individual Class members, including, without limitation:

a. whether Wawa engaged in the active misfeasance and misconduct alleged herein;

b. whether Wawa owed a duty to Plaintiffs and members of the Class to act reasonably to protect Payment Card Data;

c. whether Wawa failed to provide adequate security to protect Payment Card Data;

d. whether Wawa negligently, or otherwise improperly, allowed third parties to access Payment Card Data;

e. whether Plaintiffs and members of the Class were injured and suffered damages and ascertainable losses;

f. whether Wawa's failure to provide adequate security proximately caused Plaintiffs' and Class members' injuries;

g. whether Plaintiffs and members of the Class are entitled to damages and, if so, the measure of such damages; and

h. whether Plaintiffs and members of the Class are entitled to declaratory and injunctive relief.

67. **Typicality:** All requirements of Fed. R. Civ. P. 23(a)(3) are satisfied. Plaintiffs are members of the Class, having issued payment cards that were compromised in the Wawa Data Breach. Plaintiffs' claims are typical of the other Class members' claims because, among other things, all Class members were comparably injured through Wawa's conduct.

68. **Adequacy of Representation:** All requirements of Fed. R. Civ. P. 23(a)(4) are satisfied. Plaintiffs are adequate Class representatives because they are members of the Class and their interests do not conflict with the interests of the other members of the Class that they seek to represent. Plaintiffs are committed to pursuing this matter for the Class with the Class's collective best interests in mind. Plaintiffs have retained counsel competent and experienced in complex class action litigation of this type and Plaintiffs intend to prosecute this action vigorously. Plaintiffs, and their counsel, will fairly and adequately protect the Class's interests.

69. **Predominance and Superiority:** All requirements of Fed. R. Civ. P. 23(b)(3) are satisfied. As described above, common issues of law or fact predominate over individual issues. Resolution of those common issues in Plaintiffs' case will also resolve them for the Class's claims. In addition, a class action is superior to any other available means for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiffs and other Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Wawa, so it would be impracticable for members of the Class to individually seek redress for Wawa's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense

to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

70. **Cohesiveness:** All requirements of Fed. R. Civ. P. 23(b)(2) are satisfied. Wawa has acted, or refused to act, on grounds generally applicable to the Class making final declaratory or injunctive relief appropriate.

VI. CHOICE OF LAW

71. The common law of the Commonwealth of Pennsylvania governs Plaintiffs' negligence, negligence *per* se, and injunctive relief claims.

72. Wawa's acts and omissions discussed herein were orchestrated and implemented at its corporate headquarters in Pennsylvania and the tortious and deceptive acts complained of occurred in, and radiated from, Pennsylvania.

73. The key wrongdoing at issue in this litigation (Wawa's failure to employ adequate data security measures) emanated from Wawa's headquarters in Pennsylvania.

74. Upon information and belief, control over Wawa's POS systems and IT personnel is exercised at Wawa's headquarters in Pennsylvania. For example, Wawa demonstrated that its IT and POS system activities were based out of Pennsylvania when it sought to bolster its IT infrastructure by seeking to hire an Information Security Incident Response Junior Analyst based in Wawa, Pennsylvania, to "follow the processes and procedures necessary for the detection, response and remediation of cyber related attacks on the Wawa enterprise."[30]

75. Pennsylvania, which seeks to protect the rights and interests of Pennsylvania and other U.S. businesses against a company doing business in Pennsylvania, has a greater interest in

[30] *Wawa Information Security Incident Response Junior Analyst*, *supra* note 6.

the claims of Plaintiffs and Class members than any other state and is most intimately concerned with the outcome of this litigation.

76. Application of Pennsylvania law to a nationwide class with respect to Plaintiffs' and Class members' claims is neither arbitrary nor fundamentally unfair because Pennsylvania has a significant aggregation of contacts that creates a state interest in the claims of Plaintiffs and the nationwide Class.

77. To the extent that there is a dispute concerning choice of law, such a dispute may be briefed after substantial discovery is completed.

VII. CAUSES OF ACTION

COUNT I
Negligence
On behalf of all Plaintiffs and the Class

78. Plaintiffs incorporate by reference all preceding allegations, as though fully set forth herein.

79. Wawa owed—and continues to owe—an independent duty to Plaintiffs and the Class to use reasonable care in safeguarding their Payment Card Data to prevent fraud that results from compromised financial accounts and to discover any breach in a timely manner, so that compromised financial accounts and credit cards can be closed quickly in order to avoid or reduce the volume of fraudulent transactions. This legal duty arises under general and well-established principles of negligence, in addition to several other sources, including, but not limited to, those described below. As a legal duty, it is independent of any duty Wawa owed as a result of any purported contractual obligations.

80. Wawa has a common law duty to prevent the foreseeable risk of harm to others, including Plaintiffs and the Class. It was certainly foreseeable to Wawa that injury would result

from a failure to use reasonable measures to protect Payment Card Data and to provide timely notice that a breach was detected. It was also foreseeable that, if reasonable security measures were not taken, hackers would steal Payment Card Data belonging to millions of Wawa's customers; thieves would use Payment Card Data to make a large number of fraudulent transactions; financial institutions would be required to mitigate the fraud by cancelling and reissuing the compromised cards and paying fraudulent payment card charges; and that the resulting financial losses would be immense.

81. Wawa assumed the duty to use reasonable security measures as a result of its conduct, including but not limited to its choice to utilize networked POS systems to accept payment cards as a method of payment.

82. In addition to its general duty to exercise reasonable care, Wawa also had a duty of care as a result of the special relationship that existed between Wawa and Plaintiffs and members of the Class. The special relationship arose because financial institutions entrusted Wawa with Payment Card Data. Only Wawa was in a position to ensure that its systems were sufficient to protect against the harm to financial institutions from a data breach.

83. Wawa's duty to use reasonable data security measures also arose under Section 5 of the FTC Act, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect Payment Card Data by businesses such as Wawa. The FTC publications and data security breach orders described above further form the basis of Wawa's duty. In addition, individual states have enacted statutes based upon the FTC Act that also create a duty on the part of Wawa.

84. Wawa's duty to use reasonable care in protecting Payment Card Data arose not only as a result of the common law and the FTC Act, but also because it was bound by, and had committed to comply with, industry standards, specifically including PCI DSS.

85. Wawa breached its common law, statutory, and other duties and thus, was negligent by failing to use reasonable measures to protect Plaintiffs' Payment Card Data from the hackers who perpetrated the Data Breach and by failing to provide timely notice of the breach. Upon information and belief, the specific negligent acts and omissions committed by Wawa include, but are not limited to, some, or all, of the following:

a. failure to delete cardholder information after the time period necessary to authorize the transaction;

b. failure to employ systems and educate employees to protect against malware;

c. failure to comply with industry standards for software and POS security;

d. failure to track and monitor access to its network and cardholder data;

e. failure to limit access to those with a valid purpose;

f. failure to adequately staff and fund its data security operation;

g. failure to use due care in hiring, promoting, and supervising those responsible for its data security operations; and

h. failure to recognize that hackers were stealing Payment Card Data from its network while the Data Breach was taking place.

86. In connection with the conduct described above, Wawa acted wantonly, recklessly, and with complete disregard for the consequences.

87. Wawa was fully capable of preventing the Data Breach. Wawa knew of data security measures required or recommended by the PCI DSS, FTC, and other data security experts which, if implemented, would have prevented the Data Breach from occurring. Wawa failed to take reasonable measures to secure its system, leaving it vulnerable to a breach.

88. As a direct and proximate result of Wawa's negligence, Plaintiffs and members of the Class have or will suffer injury, including, but not limited to, cancelling and reissuing payment cards, changing or closing accounts, notifying members/customers that their cards were compromised, investigating claims of fraudulent activity, refunding or paying fraudulent charges, increasing fraud monitoring on potentially impacted accounts, and taking other steps to protect themselves and their members/customers. Plaintiffs and the Class also lost or will lose interest and transaction fees, due to reduced card usage resulting from the breach, and the cards they issued (and the corresponding account numbers) were rendered worthless.

COUNT II
Negligence *Per Se*
On behalf of all Plaintiffs and the Class

89. Plaintiffs incorporate by reference all preceding allegations as though fully set forth herein.

90. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Wawa, by failing to use reasonable measures to protect Payment Card Data. The FTC publications and orders described above also form part of the basis of Wawa's duty.

91. Wawa violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect Payment Card Data and not complying with applicable industry standards, including PCI DSS, as described in detail herein. Wawa's conduct was particularly

unreasonable given the nature and amount of Payment Card Data it obtained and stored and the foreseeable consequences of a data breach at one of the country's largest private companies, including, specifically, the immense damages that would result to consumers and financial institutions.

92. Wawa's violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence *per se*.

93. Plaintiffs and members of the Class are within the class of persons that Section 5 of the FTC Act (and similar state statutes) was intended to protect, as they are engaged in trade and commerce and bear primary responsibility for directly reimbursing consumers for fraud losses.

94. The harm that has occurred is the type of harm the FTC Act was intended to guard against. Indeed, the FTC has pursued over 50 enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiffs and the Class.

95. As a direct and proximate result of Wawa's negligence *per se*, Plaintiffs and the Class have or will suffer injury, including, but not limited to, cancelling and reissuing payment cards, changing or closing accounts, notifying members/customers that their cards were compromised, investigating claims of fraudulent activity, refunding fraudulent charges, increasing fraud monitoring on potentially impacted accounts, and taking other steps to protect themselves and their members/customers. They also lost or will lose interest and transaction fees, due to reduced card usage resulting from the breach, and the cards they issued (and the corresponding account numbers) were rendered worthless.

COUNT III
Declaratory and Injunctive Relief
On behalf of all Plaintiffs and the Class

96. Plaintiffs incorporate by reference all preceding allegations, as though fully set forth herein.

97. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, which are tortious, and which violate the terms of the federal and state statutes described herein.

98. An actual controversy has arose in the wake of Wawa's Data Breach regarding its common law and other duties to reasonably safeguard Payment Card Data. Plaintiffs allege that Wawa's data security measures were inadequate and remain inadequate. Furthermore, Plaintiffs continue to suffer injury as additional fraudulent charges may be made on payment cards it issued to Wawa's customers.

99. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Wawa continues to owe a legal duty to secure its customers' personal and financial information—specifically including information pertaining to credit and debit cards used by Wawa's customers—and to notify financial institutions of a data breach under the common law, Section 5 of the FTC Act, PCI DSS standards, its commitments, and various state statutes;

b. Wawa continues to breach this legal duty by failing to employ reasonable measures to secure its customers' personal and financial information;

c. Wawa's ongoing breaches of its legal duty continue to cause Plaintiffs harm; and

d. banks, credit unions, and other institutions that reissued payment cards and were forced to pay for fraudulent transactions as a result of the Defendant's Data Breach are legally entitled to recover the costs they incurred from Defendant.

100. The Court also should issue corresponding injunctive relief requiring Wawa to employ adequate security protocols, consistent with industry standards, to protect its customers' Payment Card Data. Specifically, this injunction should, among other things, direct Wawa to:

a. utilize industry standard encryption to encrypt the transmission of cardholder data at the POS and at all other times;

b. implement encryption keys in accordance with industry standards;

c. implement EMV technology;

d. engage third party auditors, consistent with industry standards, to test its systems for weakness and upgrade any such weakness found;

e. audit, test, and train its data security personnel regarding any new or modified procedures and how to respond to a data breach;

f. regularly test its systems for security vulnerabilities, consistent with industry standards;

g. comply with all PCI DSS standards pertaining to the security of its customers' personal and confidential information;

h. install all upgrades recommended by manufacturers of security software and firewalls used by Wawa;

i. implement an education and training program for appropriate employees regarding cybersecurity and phishing; and

j. delete its customers' credit card information immediately after obtaining authorization to process the transaction and debit card information.

101. If an injunction is not issued, Plaintiffs will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach at Wawa. The risk of another breach is real, immediate, and substantial. Simply put, monetary damages, while warranted to compensate Plaintiffs and the Class for direct, quantifiable out of pocket losses resulting from the Data Breach, do not cover the full extent of injuries suffered by Plaintiffs and the Class, which include injuries that are not readily quantifiable, such as reputational harm. Moreover, unlike the immediate financial harm suffered by Plaintiffs and the Class as a result of the Data Breach, the various policy changes and effect on strategic decision making, including the diversion of significant resources in response to the Data Breach, makes it extremely difficult, if not impossible, to quantify the overall impact of the Data Breach on Plaintiffs' long term business operations. This further establishes the irreparable nature of Plaintiffs' injury.

102. The hardship to Plaintiffs and the Class, if an injunction is not issued, exceeds the hardship to Wawa, if an injunction is issued. Among other things, if another massive data breach occurs at Wawa, Plaintiffs and members of the Class will likely incur hundreds of millions of dollars in damage. On the other hand, the cost to Wawa of complying with an injunction by employing reasonable data security measures is relatively minimal and Wawa has a pre-existing legal obligation to employ such measures.

103. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at

Wawa, thus eliminating the injuries that would result to Plaintiffs, the Class, and the millions of consumers whose confidential information would be compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the Class, respectfully request that the Court:

A. Certify the Class and appoint Plaintiffs and Plaintiffs' counsel to represent the Class;

B. Enter a monetary judgment in favor of Plaintiffs and members of the Class to compensate them for the injuries suffered, together with pre-judgment and post-judgment interest, treble damages, and penalties where appropriate;

C. Enter a declaratory judgment in favor of Plaintiffs and the Class, as described above;

D. Grant Plaintiffs the injunctive relief requested;

E. Award Plaintiffs and the Class reasonable attorneys' fees and costs of suit, as allowed by law; and

F. Award such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury of any and all issues in this action so triable.

Dated: July 13, 2020

Respectfully submitted,

CARLSON LYNCH, LLP

/s/ Gary F. Lynch

Gary F. Lynch (PA ID 56887)
Jamisen A. Etzel (PA ID 311554)

1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
Tel: (412) 322-9243
Fax: (412) 231-0246
glynch@carlsonlynch.com
jetzel@carlsonlynch.com

LOWEY DANNENBERG, P.C.
Christian Levis (admitted *pro hac vice*)
Anthony M. Christina (PA ID 322528)
One Tower Bridge
100 Front Street, Suite 520
West Conshohocken, PA 19428
Tel: (215) 399-4770
Fax: (914) 997-0035
clevis@lowey.com.com
achristina@lowey.com

HAUSFELD LLP
Jeannine M. Kenney (PA ID 307635)
325 Chestnut St #900
Philadelphia, PA 19106
Tel: (215) 985-3270
Fax: (215) 985-7201
jkenney@hausfeld.com

Interim Co-Lead Class Counsel for Financial Institution Plaintiffs

LITE DEPALMA GREENBERG, LLC
Mindee J. Reuben (PA ID 75308)
1835 Market Street
Suite 2700
Philadelphia, PA 19103
Tel: (267) 314-7980
Fax: (973) 623-0858
mreuben@litedepalma.com

Interim Liaison Counsel for Financial Institution Plaintiffs

DICELLO LEVITT GUTZLER LLC
Amy E. Keller
Ten North Dearborn Street, Eleventh Floor
Chicago, Illinois 60602

Tel: (312) 214-7900
akeller@dicellolevitt.com

GOLOMB & HONIK, P.C.
Kenneth J. Grunfeld (PA ID 84121)
1835 Market Street, Suite 2900
Philadelphia, PA 19103
Tel: (215) 985-9177
Fax: (215) 985-4169
kgrunfeld@golombhonik.com

LOCKRIDGE GRINDAL NAUEN P.L.L.P.
Karen H. Riebel (admitted *pro hac vice*)
100 Washington Avenue S, Suite 2200
Minneapolis, MN 55401
Tel: (612) 339-6900
Fax: (612) 339-0981
khriebel@locklaw.com

CHESTNUT CAMBRONNE PA
Bryan L. Bleichner (*pro hac vice* forthcoming)
100 Washington Avenue South, Suite 1700
Minneapolis, MN 55401
Tel: (612) 339-7300
Fax: (612) 336-2940
bbleichner@chestnutcambronne.com

LEVIN SEDRAN & BERMAN, LLP
Charles E. Schaffer (PA ID 76259)
510 Walnut Street – Suite 500
Philadelphia, PA 19106-3697
Tel: (215) 592-1500
Fax: (215) 592-4663
cschaffer@lfsblaw.com

THE COFFMAN LAW FIRM
Richard L. Coffman (admitted *pro hac vice*)
Edison Plaza
350 Pine Street, Suite 700
Beaumont, TX 77701
Tel: (409) 833-7700
Fax: (866) 835-8250
rcoffman@coffmanlawfirm.com

MORGAN & MORGAN COMPLEX LITIGATION GROUP
Jean S. Martin (admitted *pro hac vice*)
201 N. Franklin Street, 7th Floor
Tampa, FL 33602
Tel: (813) 559-4908
Fax: (813) 222-4795
jeanmartin@forthepeople.com

Additional Counsel for Financial Institution Plaintiffs